Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The Role of Legislation in Enhancing AI and Privacy Principles: A Comparative Look

Hala Alhaded, Ph.D.
May 13, 2025

ARTICLE INFO

Received: 24 Dec 2024

Revised: 12 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

Artificial intelligence is being applied in a variety of fields to provide several advantages. However, as it is used more, individuals are becoming concerned about their privacy, biases, and the inability to trust the technology. While there are many extensive discussions about the role of data protection laws and regulations in AI systems, this paper aims to exclusively explore the link between processes and duties. It is an attempt to unfold the areas where legislation can be seen as a tool to embed privacy principles into all processes within a still incomplete AI framework. A major theme of this paper is the fact that AI and legislative solutions are inextricably linked. It asserts that there is a role for legislation to step into the breach and up the ante for privacy protection in AI systems. There is a strong need for ongoing collaboration between policymakers and private companies responsible for developing and rolling out AI, and candid public debate about how principles should be environmentally embedded.

Keywords: Artificial intelligence, Privacy, Data protection, Legislations.

1. INTRODUCTION

Artificial Intelligence (AI) is being used in lots of different areas to bring a bunch of benefits.[1] But as it gets used more, people are getting worried about their privacy, discrimination, and not being able to trust the technology.[2] Today's tech world is so diverse and advanced that things like smart TVs, phones, watches, traffic cameras, and even fridges are always taking and sharing pictures, videos, and audio of people who never even talked to them. To this end, there's an urgent need for lawmaking that can protect people and make the companies behind these devices take responsibility. While several scholars have extensively discussed the role of data protection laws and regulations in AI systems, this paper aims to exclusively explore the link between processes and duties. It is an attempt to unfold the areas where legislation can be seen as a tool to embed privacy principles into all processes within a still incomplete AI framework. We think these ideas are really important for making sure that laws and AI systems work together well. Lawmakers will probably use these ideas when they make new rules for AI. The paper starts by looking at the importance of privacy in today's world of fast technology changes. Then it dives deeper into how data protection and AI can help each other even though they have different goals. We also talk about the idea of explaining how AI works, and how being transparent can make AI more fair and accountable. The paper ends by listing some places where AI systems are explained and suggesting ways that lawmakers can focus on including privacy in AI.

2. FOUNDATIONAL CONCEPTS

AI, particularly machine learning and deep learning, is a mechanism that allows machines to reason, learn, and act accordingly.[3] AI technologies are deemed types of intelligent systems that can rival and ultimately replace and augment human decision-making processes. This allows for the development of applications ranging from natural language processing, financial services, healthcare analytics, robotics, and recommendation systems.[4] In brief, AI

[1] Sunitha Abhay Jain, *Artificial Intelligence: A Threat to Privacy?*, 8 Nirma U. L.J. 33, 33 (2019), https://ssrn.com/abstract=3443004.
[2] Martin Ebers, *Regulating AI and Robotics: Ethical and Legal Challenges*, in *Algorithms and Law* 22, 22 (Martin Ebers ed., Cambridge Univ. Press 2019), https://ssrn.com/abstract=3392379.
[3] A.-T. Shumba et al., *Leveraging IoT-Aware Technologies and AI Techniques for Real-Time Critical Healthcare Applications*, 22 Sensors 7675, 7 (2022), https://doi.org/10.3390/s22197675.
[4] Ebers, *supra* note 2, at 23.

technologies are composed of a series of models supervised to learn the given data and use it to make decisions similar to the labeled target output. AI technologies can be classified as follows: rule-based AI (in which explicit rules are used to control the AI model that learns the rules to drive changes),[5] machine learning algorithms, and deep learning.[6] AI's growth impacts data handling practices and privacy norms to respond to advances in AI concerning accuracy and its potential impacts. This innovative sector faces several challenges, especially with the rise of automation and AI applications.[7] Challenges surrounding AI are continually under question and understanding because of its black-box-like classification regarding deep learning, due to the use of data and potential hidden bias in data and the need for high resource processing for applications such as energy, computing resources, and connectivity. Moreover, the transparency of datasets and labeled targets can lead to AI technologies' low defensibility and robustness, impacting users, industries, and broader application services.[8] There is broad recognition around the need for transparency and explanatory tools to assist end-users and customers in making informed decisions, particularly where AI technologies have been used to develop products in regulated sectors.[9] Federal legislation is in place in other countries to address these emerging issues directly, particularly with regard to bias and drift. Thus, the Privacy Act and the California Consumer Privacy Act emerged from a recognition of systemic or intentional biases that can operate on deep learning models using re-identification of anonymized data.[10] In Europe, obstacles to access continue to evolve, although relative user trust in AI technologies has not decline. [11] On some fronts, AI poses challenges and affects data privacy and privacy preferences.[12] These areas create new tiers of society affected by AI, as well as populations that embrace AI services like digital support, and generate serious concerns about dependency and model drift. Fully realizing the harmful impacts of AI-related privacy concerns may require the adoption of new legislation, which unites these issues and provides normative enforcement powers.

2.1. Artificial Intelligence (AI)

The term Artificial Intelligence (AI) was coined in 1956 and became a popular research theme in the 1970s.[13] Modern AI has been defined by its ability to replicate human intelligence while carrying out a variety of tasks.[14] There are two main types of AI: narrow AI and general AI. Narrow AI accomplishes a particular task, i.e., it can only play chess or scan business records for specific data files. In contrast, general AI is designed to abstractly reason and perform any intellectual task that a human can do.[15] AI has become an essential co-worker, co-player, co-creator, and co-decision maker for humans and has enormous potential as a game changer.[16] AI technologies cover a range of techniques, including techniques for building computational models of cognition, machine learning, expert systems, soft computing, robotics, computer vision, natural language processing, optimization, search, data mining, and computational game theory.[17] AI has led to significant growth in many areas, such as business, academic research, service and operational sectors, health care, digital devices, and social communication.

---

[5] Keyur Tripathi & Usama Mubarak, *Protecting Privacy in the Era of Artificial Intelligence* (Mar. 24, 2020), https://ssrn.com/abstract=3560047.
[6] Jain, *supra* note 1, at 33.

[7] Robert Walters & Matthew Coghlan, *Data Protection and Artificial Intelligence Law: Europe Australia Singapore - An Actual or Perceived Dichotomy*, 4 Am. J. Sci., Eng'g & Tech. 55, 55 (2029), https://doi.org/10.11648/j.ajset.20190404.11.
[8] Paul Ohm, *Changing the Rules: General Principles for Data Use and Analysis*, in *Privacy, Big Data, and the Public Good: Frameworks for Engagement* 96, 96 (Julia Lane et al. eds., Cambridge Univ. Press 2014).
[9] *Id.* at 111.
[10] Eric Goldman, *An Introduction to the California Consumer Privacy Act (CCPA)* (Santa Clara Univ. Legal Studies Rsch. Paper, July 1, 2020), https://ssrn.com/abstract=3211013.
[11] Andy Crabtree et al., *Privacy by Design for the Internet of Things* 10 (2022), https://ssrn.com/abstract=4002324.
[12] Ebers, *supra* note 2, at 23.
[13] Daniel Alexandre Bloch, *Machine Learning: Models and Algorithms* 19 (2018), https://ssrn.com/abstract=3307566.
[14]Nathan Reitinger, *Artificial Intelligence is Like a Perpetual Stew*, 73 Am. U. L. Rev. 9, 9 (2024), https://ssrn.com/abstract=4685772.
[15] Joshua Ellul et al., *Regulating Artificial Intelligence: A Technology Regulator's Perspective* 2 (June 24, 2021), https://ssrn.com/abstract=3873329.
[16] Ishaq Azhar, *How Artificial Intelligence Is Changing Cyber Security Landscape and Preventing Cyber Attacks: A Systematic Review*, 4 Int'l J. Creative Rsch. Thoughts 659, 660 (2016), https://ssrn.com/abstract=3905773.
[17] Jain, *supra* note 1, at 35.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

AI operations are carried out based on the immeasurable amounts of data collected from various devices and sources.[18] Many countries refer to AI as the new "electricity" that sparks economic development in many sectors. AI is the core part of the big data ecosystem;[19] however, there is no single definition or threshold for big data.[20] AI is emerging as a technology that processes such massive and diverse datasets at a rapid speed. It builds smart models for decision making and can perform such tasks with more accuracy and reliability than humans can. The rapid transformation of technology has the potential to revolutionize the management of personal data. Data protections and privacy laws, including regulations within democratic countries, relate to the protection of physical individuals regarding the processing of personal data.[21] Therefore, regulations regarding the AI system for the digital data systems used in such organizations must be exercised cautiously.[22] As AI is dependent on the use of data, any renewal and regulation should be seen as a means to improve human rights in the digital ecosystem by making the data protection principles more stringent when such data are processed by AI. Modern AI includes advanced data storage technologies and sophisticated algorithms and techniques based on neural networks, blockchain, and quantum computing. Neural networks are one of the main tools for an AI agent that can be trained with large and diverse datasets.[23] This allows the AI agent to recognize patterns or trends in a novel dataset and make decisions accordingly. However, one of the major challenges of AI development is to manage the risks related to the use of untrustworthy inputs and outputs. Many researchers are doing work related to the performance and accuracy of these machine learning techniques,[24] but less has been done in the sphere of data protection and privacy. Aside from this, four concerns emerge from the training and testing of AI systems that are discussed below.

Development in neural networks such as spiking neural networks,[25] convolutional neural networks,[26] and long short-term memory are closely related to the processing of personal data. The AI system analyzes and makes decisions whenever any portion of the data is personally related to an individual, such as image data, geolocation data, speech, telecommunication, facial identity, health data, and email.[27] Artificial intelligence is the future of the technological world; but like everything good, it is a gift as well as a curse. Data protection is a fundamental right in any democratic country, but recent technological transformations in the digital privacy era contribute to a potential breach in data protection and in the special protection of children, confidentiality, digital privacy, big data, social media, and guidelines that are the cornerstone within the data protection regulation discussed.[28]

3. CURRENT PRIVACY CONCERNS

AI, encompassing machine learning, neural networks, and natural language processing, among others, has given rise to a wealth of privacy concerns.[29] AI manipulates, analyzes, and processes information in big data, which includes websites visited, social media posts, watch history, photos and videos taken, and locations visited. An estimated 1.7

[18] Ebers, *supra* note 2, at 22.
[19] *Id.* at 23.
[20] Walters & Coghlan, *supra* note 7, at 59.
[21] Jain, *supra* note 1, at 33.
[22] Walters & Coghlan, *supra* note 7, at 55.
[23] Anusha S, *Basic of Artificial Neural Network Overview*, 2 Cent. Asian J. Mathematical Theory & Comput. Sci. 87, 87 (2021), https://ssrn.com/abstract=3971265.
[24] Bloch, *supra* note 13, at 19–20.
[25] Mingqi Yin et al., *A Reconfigurable FPGA-Based Spiking Neural Network Accelerator* 1 (2024), https://ssrn.com/abstract=4876812.
[26] Sara Shomal Zadeh et al., *Concrete Surface Crack Detection with Convolutional-Based Deep Learning Models*, 10 Int'l J. Novel Rsch. Civ. Structural & Earth Sci. 25, 25 (2023), https://ssrn.com/abstract=4661249.
[27] Karl M. Manheim & Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 Yale J.L. & Tech. 106, 120 (2018), https://ssrn.com/abstract=3273016.
[28] Tripathi & Mubarak, *supra* note 5.
[29] Ebers, *supra* note 2, at 8.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

MB of data for every person on the planet is produced every second.[30] Immoral uses include email scams, disseminating child abuse, stalking, doxxing, scam dialing, and deepfakes.[31] Firms use browsing data, credit history, race, age, and criminal histories to assess credit ratings, job suitability, and even arrest probability by police.[32] Finally, many sites gain consent to collect data by a false choice.[33]

The greatest quandary is the lack of transparency in many data practices. Collecting companies seldom tell customers how they employ data. People are sometimes kept in the dark if data is shared, repurposed, or sold on. Many websites and apps produce personal data not only from user interactions but also by taking web activity from the web browser activities or device. Small increases in public interest are registered on how AI is used, and an overwhelming 93% of the population hope most firms can be held liable for their utilization of AI technology. Data breaches are a significant risk, as exemplified by unauthorized access to about 87 million users in a major breach, the 2017 database hack, among many others. It is noteworthy that privacy law has not kept pace with technological advancements and does not even completely protect other privacy interests. As stated, to a large extent, AI is yet a nascent and evolving technology. Governments, including policymakers, should act with foresight to provide a strong and flexible AI regulatory framework that can readily accommodate inevitable changes. The durability and trustworthiness of AI and digital sectors will be built on privacy laws and other norms to consent to individual autonomy and assuage adverse AI-related rhetoric.

The intersection of artificial intelligence and data privacy presents an intricate legal conundrum that remains insufficiently addressed within existing regulatory frameworks. The pervasive deployment of AI in data processing, behavioral analytics, and automated decision-making challenges foundational legal doctrines, particularly those concerning autonomy, consent, and due process. Contemporary legal instruments, including data protection statutes and consumer privacy laws, are often retroactive rather than anticipatory, failing to account for AI's unprecedented capacity to aggregate, infer, and repurpose personal data. This lacuna in legal oversight creates a landscape in which corporate entities and state actors operate with a level of impunity, leveraging AI's opacity to circumvent traditional accountability structures. The doctrine of informational self-determination, which affirms an individual's right to control their personal data, is continually eroded by the seamless and often covert integration of AI into digital ecosystems.

A particularly problematic facet of AI-driven data collection is the systemic obfuscation of its methodologies. The principle of transparency, a cornerstone of legal proceduralism, is fundamentally incompatible with the opaque nature of many AI models, particularly those employing deep learning and neural networks. Algorithmic opacity effectively precludes meaningful consent, rendering existing legal requirements for disclosure and affirmative agreement largely illusory. Furthermore, AI's propensity for adaptive learning exacerbates concerns related to the perpetuation of bias, the reinforcement of discriminatory decision-making, and the erosion of due process rights. The absence of robust mechanisms for algorithmic interpretability and oversight raises profound legal and ethical concerns, particularly in domains where AI systems exert significant influence over individual liberties, such as employment eligibility, financial access, and criminal justice assessments.

The jurisprudential response to AI's encroachment on privacy and data rights must be both dynamic and preemptive. A rigid, reactive regulatory approach is insufficient to address the fluid and evolving nature of AI technologies. Instead, legal frameworks must embrace a principles-based approach, integrating substantive due process protections, enhanced fiduciary duties for data controllers, and sector-specific AI governance norms. The

---

[30] Reyell, *How Much Data Is Produced Every Day?*, Ne. Univ. Graduate Programs (2024), https://graduate.northeastern.edu/knowledge-hub/how-much-data-produced-every-day/ (last visited Jan. 30, 2025).

[31] Julia M. Puaschunder, *The Legal and International Situation of AI, Robotics and Big Data with Attention to Healthcare* 16 (2019), https://ssrn.com/abstract=3472885.

[32] *Id.* at 1–3.

[33] Walters & Coghlan, *supra* note 7, at 60.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

introduction of algorithmic accountability measures, including mandatory impact assessments, explainability standards, and independent oversight bodies, would serve as essential safeguards against unchecked AI expansion. Furthermore, the legal concept of harm in the context of AI privacy violations must be reconceptualized to recognize not only tangible economic damages but also broader dignitary harms arising from surveillance, data commodification, and digital profiling.

Beyond domestic legal reform, the extraterritorial nature of AI and data flows necessitates a harmonized, transnational regulatory framework. The current jurisdictional fragmentation, wherein data protection laws vary widely across legal systems, facilitates regulatory arbitrage and undermines efforts to impose meaningful constraints on AI-driven data exploitation. The development of an international AI governance regime, akin to the existing frameworks for human rights and financial regulation, is imperative to ensure that privacy protections are not contingent upon geographic happenstance. Only through a sophisticated, anticipatory, and enforceable legal architecture can AI be reconciled with the fundamental tenets of privacy, autonomy, and human dignity.

3.1. Data Collection and Usage

One major issue of AI research and development is the large amount of data required to make systems work. While there are possible techniques to work around such a requirement, large-scale data collection efforts have become common in the field. These collection practices may not pass ethical or legal considerations, which have led to an urgent need for broader regulation of businesses specifically to address these privacy-invading practices.[34]

There are several common methods for an AI or system to collect data. These general techniques include passive collection, such as with cookies, [35] and active collection, where the company explicitly asks for the relevant data.[36] It should be noted that data collection is not inherently problematic if it satisfies some key criteria. The first and typically most important criterion is whether the data is collected in a way that has been consented to.[37] Informed consent is an important part of privacy to ensure individuals know what will be done with their data and by whom. Without consent, there may be no legal basis for collection and usage, and the system architecture may actually breach laws.[38] It is worth highlighting again in this context the concept of explicit consent, where there is a need for an explicit, affirmative action to give consent; simply having poor options to opt-out (or none) will be insufficient.

Another important consideration is the ownership of the data and the protection of the rights of the people providing that data.[39] For the complexity of this topic and the ongoing discussion, for the purpose of this paper, we describe those that provide their data as the owners. This allows a rights-based approach that can be used to protect their data from unauthorized or deceptive collection efforts. Data harvesting or scraping of personal data has already occurred in relation to stalking, where the data is collected and reused to an unlawful extent. Exploitation of this nature must be regulated to prevent similar actions using such systems. Even with these factors in mind, it is important to handle such limitations on usage correctly, as their use in an overbearing way could lead to an isolated AI ecosystem, one primarily dominated by global players that have the resources to do something that is possibly unanticipated and border-free. At the same time, removal of these options entirely may inhibit and dampen industry innovation in AI. In this double-edged context, the need to regulate AI-producing companies, including local ones, now appears urgent and, regardless of the wider debate, should occur to support the idea that individuals have a fundamental right to privacy.[40]

---

[34] *Id.* at 55.
[35] Paul Wagner, *Cookies: Privacy Risks, Attacks, and Recommendations* 2 (Univ. of Ariz. Coll. of Applied Sci. & Tech., Dec. 8, 2020), https://ssrn.com/abstract=3761967.
[36] Graham Greenleaf et al., *Implementing Privacy Principles: After 20 Years, It's Time to Enforce the Privacy Act* (UNSW Law Rsch. Paper No. 2007-31, May 20, 2007), https://ssrn.com/abstract=987763.
[37] Christof Koolen, *Transparency and Consent in Data-Driven Smart Environments*, 6 Eur. Data Prot. L. Rev. 174, 186 (2020), https://ssrn.com/abstract=3597736.
[38] Ohm, *supra* note 8, at 116.
[39] Ebers, *supra* note 2, at 22–23.
[40] Greenleaf et al., *supra* note 36, at 14.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The legal and ethical implications of large-scale data collection for AI development remain a contentious issue, underscoring the need for a nuanced regulatory response. AI systems, by their very nature, require vast amounts of data to function effectively, prompting companies to engage in extensive data collection practices that often skirt the boundaries of legality and ethical acceptability. The principle of informed consent, a cornerstone of data protection law, is frequently undermined by ambiguous or manipulative consent mechanisms that fail to provide individuals with a meaningful choice over the use of their data. In many instances, the sheer asymmetry of information between data subjects and collectors renders any purported consent illusory, raising significant legal concerns regarding the validity of such arrangements. Where consent is not explicit, affirmative, and freely given, data collection may not only be ethically problematic but may also contravene established privacy laws and fundamental rights.

Beyond consent, the legal construct of data ownership remains an area of considerable ambiguity. While the notion that individuals retain ownership over their personal data aligns with broader privacy rights, existing legal frameworks are often insufficient to enforce such claims effectively. The unauthorized or deceptive harvesting of personal data—whether through passive means such as cookies or active solicitation—raises fundamental questions about control, agency, and accountability. In cases where AI systems collect and process personal data without clear legal justification, such practices may constitute unlawful surveillance or even data exploitation. This is particularly concerning in the context of AI-driven profiling, where individuals may be subjected to automated decision-making without their knowledge or recourse. The principle of data sovereignty must therefore be reinforced within legal frameworks to ensure that individuals maintain not only theoretical but also enforceable rights over their personal information.

The intersection of AI regulation and data governance also presents challenges in balancing innovation with individual rights. Overly restrictive regulations could risk stifling AI development, consolidating power within a handful of dominant global entities with the resources to navigate complex legal landscapes. Conversely, an unregulated AI ecosystem would leave individuals vulnerable to unchecked data exploitation, reinforcing the need for a calibrated legal approach. The concept of proportionality must be at the heart of any AI regulatory framework, ensuring that privacy protections do not inadvertently create monopolistic conditions while also safeguarding against mass data commodification. This necessitates the implementation of sector-specific legal standards, robust enforcement mechanisms, and oversight structures that hold data collectors to account while fostering a responsible and competitive AI industry.

At an international level, the borderless nature of data flows and AI development calls for greater harmonization of privacy and AI governance laws. Current jurisdictional fragmentation allows companies to engage in regulatory arbitrage, operating under the least restrictive legal regimes while continuing to exploit user data on a global scale. The establishment of an international framework for AI governance—one that upholds privacy as a fundamental right—remains an urgent priority. Such a framework must integrate principles of transparency, accountability, and data protection by design, ensuring that AI-producing entities operate within legal and ethical boundaries irrespective of their geographical location. Only through a sophisticated and enforceable legal architecture can AI-driven data collection be reconciled with the fundamental tenets of individual autonomy, privacy, and digital rights.

4. EXISTING LEGISLATION AND REGULATIONS

Existing legislation and regulations play a pivotal role in governing the interplay between AI technologies and privacy principles.[41] Depending on the country in which an AI system is developed, implemented, or deployed, different legislation and regulations exist. In addition to national laws, numerous international agreements touch on AI technologies or on the specific areas in which AI systems are applied, including privacy. At a general level, three international agreements are of key relevance when discussing the international protection of personal data: the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights.[42] These agreements

[41] Jain, *supra* note 1, at 35.

[42] Christopher Kuner, *International Organizations and the EU General Data Protection Regulation: Exploring the Interaction Between EU Law and International Law*, 16 Int'l Orgs. L. Rev. 158, 161 (2018), https://ssrn.com/abstract=3050675.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

are broad and general. They set out legal principles at a high or broad level of generality and are not directly connected to AI regulation.[43]

At a more specific level, international agreements have been developed that deal more directly with privacy. The European Union's regulation: The General Data Protection Regulation GDPR has been a leader in this regard. The GDPR has become a de facto standard for regulating privacy, with around 120 countries around the world having implemented or working towards adopting new national privacy laws.[44] These privacy laws are modeled on the GDPR and are highly prescriptive, limiting the uses of personal data by AI technologies when the personal data has been collected for a significant body of EU-led privacy.[45] Many legal scholars and privacy advocates consider the GDPR not only the most advanced privacy law but also the most advanced legislation globally for regulating AI.[46] However, AI privacy legislation is not just an EU issue. The US and other countries have begun developing and implementing AI-relevant privacy legislation. These privacy laws also limit certain uses of personal data when the personal data was collected for non-AI purposes. Some require individuals' consent for the specific, time-bound use of personal data in AI models. Other AI-relevant privacy laws are less prescriptive than the GDPR and focus on transparency, individual rights, and accountability for AI-based privacy violations.[47] Some countries have chosen to commit to the OECD AI principles, which contain provisions specifically focused on privacy.[48] Today, most of the world's largest social media, search, and e-commerce companies operate in markets with AI and privacy regulations. However, subject to particular variations that reflect the diverse regulatory ideologies and principles of different jurisdictions, international laws regulating the area of privacy share a series of commonalities.[49]

However, the criticisms of existing laws, including privacy laws, in addressing the challenges arising in the AI environment are numerous and weighty.[50] For example, existing laws often rely on individuals' awareness of potential issues and their capacity to take measures to address them. The affordances and constraints of AI make it challenging to fulfill this basic assumption of individual empowerment. AI-based decisions often rely on a variety of data, including previous choices, about what steps users have taken. It is impossible for individuals to have knowledge of the full scope of data and analyses used to support AI-based decisions, its underlying details, its normative basis, and its intended and unintended uses.[51] In addition, since decisions about individuals are, in some cases, fundamentally unknowable to individuals, it is challenging to evaluate the accuracy, validity, or fairness of final decisions made by AI systems. Finally, individuals, no matter how well-informed and empowered, may not be able to effectively challenge AI-supported administrative decisions.[52]

The evolving legal landscape surrounding AI and privacy is deeply intertwined with existing legislative frameworks and international agreements. While various national and supranational regulations attempt to govern AI's interaction with privacy rights, the adequacy and efficacy of these laws remain contentious. Foundational international human rights instruments, such as the *Universal Declaration of Human Rights* (UDHR) and the *International Covenant on Civil and Political Rights* (ICCPR), articulate broad principles that underpin privacy protections.[53] However, these instruments, while significant, lack the specificity required to address the novel and

[43] *Id.* at 161.
[44] Alexander Wodi, *The EU General Data Protection Regulation (GDPR): Five Years After and the Future of Data Privacy Protection in Review* 3 (2023), https://ssrn.com/abstract=4601142.
[45] Samuel Goldberg et al., *Regulating Privacy Online: An Economic Evaluation of the GDPR*, 16 Am. Econ. J.: Econ. Pol'y 325, 325 (2019), https://ssrn.com/abstract=3421731.
[46] Josephine Wolff et al., *Lessons from GDPR for AI Policymaking*, 27 Va. J.L. & Tech. 1, 1–2 (2023), https://ssrn.com/abstract=4528698.
[47] Mohamed ElBaih, *The Role of Privacy Regulations in AI Development* 30 (Geo. Wash. Univ. L. Sch., Apr. 1, 2023), https://ssrn.com/abstract=4589207.
[48] *Id.* at 45.
[49] *Id.* at 65–67.
[50] Walters & Coghlan, *supra* note 7, at 59.

[51] Ebers, *supra* note 2, at 25.
[52] Ohm, *supra* note 8, at 109–10.
[53] G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948), https://www.un.org/en/about-us/universal-declaration-of-human-rights; International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

complex challenges posed by AI-driven data collection, processing, and decision-making. The rapid advancement of AI has outpaced traditional regulatory mechanisms, necessitating a more targeted approach to data governance that accounts for AI's unprecedented capacity for autonomous and large-scale information processing.

The *General Data Protection Regulation* (GDPR) of the European Union has emerged as the most influential legal instrument shaping AI and privacy law.[54] Its extraterritorial applicability and stringent requirements for data processing, informed consent, and individual rights have set a de facto global standard. More than 120 jurisdictions have either adopted or are in the process of aligning their national privacy laws with GDPR principles, reflecting its far-reaching impact. The regulation establishes rigorous accountability measures for AI-driven data processing, prohibiting the use of personal data beyond its original purpose unless explicit and specific consent is obtained.[55]Furthermore, GDPR enshrines individuals' rights to explanation and redress in cases of automated decision-making, imposing legal obligations on AI developers and deployers to ensure transparency, fairness, and non-discrimination in algorithmic processing.[56]

Despite the GDPR's comprehensive framework, AI privacy regulation remains highly fragmented across jurisdictions. The United States, for instance, lacks a federal AI privacy law analogous to the GDPR, instead relying on sector-specific and state-level regulations that prioritize transparency and accountability over prescriptive limitations on data use. Other jurisdictions, including Canada, Japan, and Australia, have adopted hybrid approaches, combining elements of GDPR-like data protection with AI-specific oversight mechanisms.[57] Meanwhile, initiatives such as the *OECD AI Principles* offer a voluntary framework that emphasizes AI ethics, privacy, and human rights, yet lack binding enforcement provisions.[58] The absence of a unified global AI privacy regime allows for regulatory arbitrage, where corporations strategically operate in jurisdictions with weaker privacy protections to maximize data exploitation while minimizing legal exposure.

A significant criticism of existing privacy laws, including the GDPR, is their reliance on individual awareness and proactive engagement in protecting personal data. In the AI context, this assumption is fundamentally flawed, as individuals are often unable to comprehend the full extent of data collection, processing, and decision-making involved in AI systems. AI operates through layers of data integration and machine learning processes that are opaque even to their developers, let alone the average data subject. This lack of transparency creates substantial barriers to meaningful consent and effective oversight, rendering many existing legal provisions insufficient in practice. The inability of individuals to assess the validity, accuracy, and fairness of AI-driven decisions—especially in high-stakes contexts such as employment, credit scoring, and law enforcement—further underscores the inadequacy of the current regulatory paradigm.

Moreover, legal mechanisms for redress in AI-driven administrative and commercial decision-making remain underdeveloped. Even in jurisdictions with robust data protection laws, individuals face structural disadvantages when attempting to challenge AI-generated outcomes. The complexity and proprietary nature of many AI models impede efforts to scrutinize decision-making processes, leaving individuals with limited recourse to contest adverse determinations. This systemic asymmetry in power and information calls for the establishment of independent oversight authorities with technical expertise in AI governance, empowered to audit, assess, and regulate AI systems in a manner that prioritizes fundamental rights.

---

[54] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, https://gdpr.eu/tag/gdpr/.
[55] *Id.*
[56] *Id.* art. 71.

[57] Mike Woodward, *16 Countries with GDPR-like Data Privacy Laws*, SecurityScorecard (July 8, 2021), https://securityscorecard.com/blog/countries-with-gdpr-like-data-privacy-laws/.
[58] OECD Principles on Artificial Intelligence, OECD/LEGAL/0449 (May 22, 2019), https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

As AI continues to permeate all facets of modern life, the need for a harmonized, enforceable, and forward-looking legal framework becomes ever more urgent. A mere adaptation of existing data protection laws will be insufficient to address the unique challenges AI poses to privacy and human autonomy. Instead, a paradigm shift in regulatory thinking is required—one that integrates AI-specific accountability mechanisms, ensures algorithmic explainability, and reinforces the principle that privacy is not merely a transactional commodity but a fundamental right that must be preserved in the digital age.

4.1. General Data Protection Regulation (GDPR)

Again, the GDPR is a fundamental legislative framework adopted by the European Parliament and Council in April 2016. The European Union Act on the General Data Protection Regulation came into force on May 25, 2018, and has a direct and general application from this date onwards.[59] The GDPR contains several provisions to safeguard personally identifiable data, augmenting individual privacy rights and providing individuals with workable control and permission over their personal data.[60] The data collection principle that interferes with the privacy of an individual is data minimization.[61] Therefore, Article 5 of the GDPR engages the controller not to accumulate personal data more than required for the determination and should be stored for a limited time.[62] Other general privacy principles specified by the GDPR embody transparency, accuracy, consent, openness, purpose limitation, and data security.[63] The use and deployment of AI should adhere to the conditions mentioned in these principles. Article 35 of the GDPR requires the performance of a Data Protection Impact Assessment concerning all-conclusive AI technologies to prevent the exposure of privacy. The GDPR reasserts the static principles of privacy set forth in 1995 and emphasizes the area where the guidelines are newly implemented by providing an extended disclosure on transparency and individual control, such as user-based consent, the right of access, and the erasure of an individual's data.[64]

Data Protection by Design and by Default: The core elements of the GDPR encompass privacy by purpose, data collection, data storage, data security, and lawfulness of data processing.[65] GDPR Article 25 obligates data controllers, whether acting alone or collectively with others, to appoint the goals and means for processing personal data and to have the appropriate technical and managerial measures, such as encryption and pseudonymization, and to integrate the necessary safeguards and privacy-enhancing technologies into their processing activities by default, in such a manner that the processing of personal data does not exceed what is needed for the purpose of data collection and complies with data security. Therefore, the technical AI systems comply with the GDPR, which describes the data protection requirements involving AI technologies and decisions taken by a data controller that establish the storage periods for personal data.

The GDPR stands as a cornerstone of contemporary data protection law, embodying a comprehensive legal framework that governs the collection, processing, and storage of personal data within the European Union and beyond. Enacted by the European Parliament and Council in April 2016 and taking full effect on May 25, 2018, the GDPR establishes a direct and uniform regulatory standard across EU member states, effectively reshaping global data protection practices. The regulation is not merely a codification of pre-existing privacy principles but a transformative legal instrument that strengthens individual rights, enhances transparency, and imposes stringent obligations on data controllers and processors. Central to its mandate is the concept of *data minimization*, enshrined in Article 5, which prohibits the excessive accumulation of personal data and mandates that such data be retained only for as long as necessary for its lawful purpose. This principle is particularly consequential for AI-driven data

[59] Greenleaf et al., *supra* note 36, at 5, 10.
[60] Ohm, *supra* note 8, at 108.
[61] *Id.* at 108.

[62] Regulation 2016/679, *supra* note 54, art. 5.

[63] *Id.* art. 5(1)(a).
[64] ElBaih, *supra* note 47, at 32.
[65] *Id.* at 33–34.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

processing, where indiscriminate data collection is often an inherent feature, necessitating strict adherence to GDPR constraints.

A defining feature of the GDPR is its reinforcement of traditional privacy doctrines while introducing novel safeguards specifically tailored to modern digital and algorithmic ecosystems. Transparency, accuracy, purpose limitation, and data security form the bedrock of GDPR compliance, ensuring that AI-driven technologies operate within well-defined ethical and legal boundaries.[66] Article 35 introduces a requirement for *Data Protection Impact Assessments* (DPIAs) for AI applications that pose significant risks to individual privacy, compelling organizations to evaluate the implications of their data practices before deployment. This preemptive approach represents a fundamental shift in privacy governance, obligating AI developers and deployers to proactively assess and mitigate potential privacy risks rather than merely responding to breaches or regulatory violations post facto.[67] The GDPR thus transcends static privacy principles, incorporating dynamic regulatory tools that impose continuous oversight and accountability on AI-based decision-making processes.

An essential innovation within the GDPR framework is the principle of *Data Protection by Design and by Default*, articulated in Article 25.[68] This provision mandates that privacy-enhancing measures be integrated into AI systems at the design stage rather than retrofitted as an afterthought. It imposes obligations on data controllers to implement technical and organizational measures—such as encryption, pseudonymization, and access controls—that restrict data processing to what is strictly necessary for the intended purpose. This principle not only limits unnecessary data retention but also fortifies AI-driven systems against unauthorized access, misuse, or breaches. Importantly, it aligns with broader AI governance concerns, ensuring that automated decision-making processes incorporate built-in safeguards that preserve individual autonomy and prevent excessive data exploitation.

The GDPR's emphasis on user-centric control is further exemplified through the rights it affords data subjects, including the *right to access*, the *right to rectification*, and the *right to erasure* (commonly known as the "right to be forgotten"). These provisions significantly enhance individuals' ability to oversee and regulate the use of their personal data, thereby counteracting the traditional imbalance of power between data subjects and AI-driven platforms. Moreover, the requirement for explicit and informed consent, as opposed to implied or opt-out mechanisms, reinforces the principle that data subjects must actively and knowingly authorize the use of their personal information. This has profound implications for AI technologies that rely on extensive datasets, as it limits the capacity for companies to amass and process data without clear and specific consent.

Despite its robust privacy protections, the GDPR presents both challenges and ambiguities in its application to AI. While it provides a legal framework to constrain AI-based data processing, the regulation does not fully address the complexities of AI opacity, algorithmic decision-making, and automated profiling. Questions persist regarding how the *right to explanation* can be effectively enforced in AI-driven systems where decision-making processes are inherently opaque. Additionally, the regulation's applicability to AI models trained on vast, anonymized datasets remains a subject of legal and ethical debate, raising concerns about the tension between privacy rights and technological innovation.

Nevertheless, the GDPR remains the most sophisticated and far-reaching legal instrument regulating AI's intersection with data privacy. Its extraterritorial reach has influenced jurisdictions worldwide, shaping legislative efforts in numerous countries seeking to implement GDPR-like protections. As AI continues to evolve, the principles enshrined in the GDPR will likely serve as the foundation for future regulatory frameworks, reinforcing the imperative that technological advancements must remain firmly rooted in legal accountability and the protection of fundamental privacy rights.

[66] Regulation 2016/679, *supra* note 54, ch. 2.
[67] *Id.* art. 35.
[68] *Id.* art. 25.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5. PROPOSED LEGISLATION FOR AI AND PRIVACY ENHANCEMENT

As the predominant unit of focus, data has unrivaled potential to be used and abused for various operational ends.[69] Personal data has been defined, leveraged, collected, analyzed, distributed, and capitalized upon in countless ways across various time periods, industries, and regulatory climates.[70] While data protection regulations have been implemented in various degrees of stringency across the world, new data-driven technologies pose unique challenges to these principles, including artificial intelligence and its derived technologies.[71]

Policymakers may consider multiple channels in addressing the intersection of privacy and AI. Such efforts may draw from prior experiences with policy shaping across several approaches. A static form of regulation captures the ex ante, up-front legislative route to policymaking.[72] This, however, may prove cumbersome and infeasible given the rapid rate of technological iteration and market-based innovation. The opposite route towards a "self-regulatory" regime tends to represent the inverse tendency by focusing on how stakeholders may police themselves. A compromissorial approach may be adopted, particularly one that incorporates the principle of "privacy by design" into legislative frameworks. In doing so, best privacy practices will be intrinsically embedded into technological design. Such proactive measures will unite government agencies, private industry, and social advocates in a preventive process of technical, legal, and ethical coordination.

In bolstering privacy protection across all forms of AI, a legislative body might carve out a suite of privacy dictates tailored to the unique challenges, threats, and solutions of AI. This subtext of legislation can make real a proactive approach to privacy threat mitigation. By merging principles from the public and private spheres, cooperation among diverse fields may actually keep data handlers ahead of AI innovation.[73] There is much justification for cooperation, as the huge impact of this legislative task goes far beyond borders. International cooperation would effectively manifest the agreed-upon level of global anxiety and responsibility concerning the current state of data and privacy.[74] Consequently, global protocols would enhance the speed and breadth of data sharing, with potentially disastrous misuse. However, the prevailing pace of data-rich innovation heightens the need to preventively legislate and draw from existing international privacy collaborations for timely regulatory results.

The centrality of data in the modern digital economy has positioned it as both an invaluable asset and a potential instrument of exploitation. The unprecedented scale at which personal data is collected, processed, and monetized—particularly within the context of artificial intelligence—has intensified longstanding debates regarding privacy, ownership, and regulatory oversight. While historical regulatory frameworks have sought to curtail the unchecked commodification of personal information, the advent of AI has introduced novel challenges that transcend traditional conceptions of data protection. The dynamic and evolving nature of AI-driven analytics, predictive modeling, and automated decision-making necessitates a recalibration of legal and ethical standards to ensure that privacy remains a fundamental right rather than a mere policy consideration.

The regulatory response to AI's impact on privacy must balance the need for legal certainty with the inherent fluidity of technological progress. Policymakers have historically oscillated between two extremes: rigid, ex-ante legislative approaches that risk obsolescence in the face of rapid innovation, and laissez-faire self-regulation, which often devolves into corporate opportunism absent meaningful enforcement. Neither extreme is sufficient to address the

[69] Matthijs M. Maas, *AI is Like… A Literature Review of AI Metaphors and Why They Matter for Policy* 6 (AI Founds. Rep. 2, Oct. 25, 2023), https://ssrn.com/abstract=4612468.
[70] Manheim & Kaplan, *supra* note 27, at 120.
[71] Jain, *supra* note 1, at 35–36.
[72] Robert Mahari & Alex Pentland, *Regulation by Design: A New Paradigm for Regulating AI Systems*, in *Digital Single Market and Artificial Intelligence: AI Act and Intellectual Property in the Digital Transition* 432, 432 (M. Franzosi et al. eds., Aracne 2024), https://ssrn.com/abstract=4753029.

[73] Kelsey Finch & Omer Tene, *Smart Cities: Privacy, Transparency, and Community*, in *Cambridge Handbook of Consumer Privacy* 133, 133–34 (Evan Selinger et al. eds., 2018), https://ssrn.com/abstract=3156014.
[74] Matthijs M. Maas, *Aligning AI Regulation to Sociotechnical Change*, in *Oxford Handbook on AI Governance* 3 (Justin Bullock et al. eds., Oxford Univ. Press forthcoming 2022), https://ssrn.com/abstract=3871635.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

intricate and evolving threats posed by AI. A hybrid regulatory model—one that embeds the principle of *privacy by design* into both legal and technological frameworks—presents a more viable path forward. This approach would require that privacy safeguards be proactively integrated into AI architectures from inception rather than retrofitted in response to regulatory scrutiny or public backlash. Such a framework necessitates collaboration between government agencies, private industry, and civil society, ensuring that privacy considerations are not subordinated to market imperatives.

In constructing AI-specific privacy regulations, legislative bodies must recognize the unique vulnerabilities that AI technologies introduce. Unlike conventional data-driven systems, AI possesses the capacity for autonomous learning, adaptation, and inference, often processing vast datasets in ways that elude direct human oversight. This necessitates a legislative substructure that not only mandates transparency and accountability but also preemptively mitigates privacy risks through enforceable safeguards. The convergence of legal and technological solutions—ranging from algorithmic audits and explainability standards to differential privacy techniques—can ensure that AI systems operate within ethical and legal confines. Moreover, the implementation of stringent data governance protocols, including explicit limitations on data retention, repurposing, and sharing, can prevent AI from being weaponized as a tool of surveillance, discrimination, or commercial exploitation.

Given AI's inherently transnational nature, the regulatory discourse cannot be confined to isolated jurisdictions. The cross-border flow of data, coupled with the global proliferation of AI applications, underscores the necessity of international cooperation in shaping privacy norms. A harmonized, multilateral regulatory framework would not only facilitate interoperability between different legal systems but also reinforce collective accountability in managing AI's privacy risks. Existing international agreements on data protection, such as the European Union's GDPR and the *OECD AI Principles*, provide a foundation upon which broader regulatory collaborations may be constructed. However, the urgency of AI-driven privacy concerns demands that these frameworks be expanded and adapted to address the specific challenges posed by autonomous data processing systems.

While the acceleration of AI innovation presents both economic and societal benefits, it simultaneously necessitates a more vigilant and preemptive legislative stance. The failure to implement timely and adaptive regulatory measures risks exacerbating existing privacy vulnerabilities, deepening the asymmetry of power between individuals and data controllers. The convergence of public and private sector efforts in shaping AI governance will be instrumental in ensuring that privacy remains a protected right rather than an expendable commodity. Only through proactive, enforceable, and globally coordinated legislative efforts can AI be harnessed in a manner that aligns with the principles of data dignity, autonomy, and legal accountability.

5.1. Ethical AI Frameworks

Proponents of the co-regulation approach to AI legislation suggest that proposed legislation will be implemented in conjunction with ethical AI frameworks.[75] Ethical AI frameworks are codes comprised of ethical AI principles, backed by best practice guidelines and industry audit processes.[76] These principles guide the ethical, responsible, and fair use of AI, as well as identify areas with legal risk.[77] Ethical AI principles have variances in their formation.[78] The European Commission provides a framework for ethical AI, which hinges on three guiding principles: fairness, accountability, and transparency.[79] These principles are based on the assumption that these values will, if pursued throughout businesses and society, build trust among consumers and foster organizational sustainability.[80]

[75] S. Dell et al., *Aligning Artificial Intelligence with Ethical Accountancy: A Global Perspective on Emerging Frameworks*, 21 Corp. Ownership & Control 47, 50 (2024), https://doi.org/10.22495/cocv21i1art5.
[76] *Id.* at 49.
[77] Finch & Tene, *supra* note 73, at 133–34.
[78] Dell et al., *supra* note 75, at 49.
[79] Sean Musch et al., *The EU AI Act: A Comprehensive Regulatory Framework for Ethical AI Development* 6–7 (Aug. 23, 2023), https://ssrn.com/abstract=4549248.
[80] *Id.* at 4.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Stakeholder involvement is central to international and domestic regulatory discourse. The inclusion of ethical principles in the implementation of a data protection regime is raised, as there is potential for AI to negatively impact privacy. The GDPR-focused AI reform process could demonstrate how principles are already embedded into privacy laws and create harmonized goals for future AI reform.[81] Some ethical AI reforms assert the importance of the principles being consistent with existing privacy law to ensure stronger data privacy regulation. While the European Commission AI strategy aims for AI leadership with simultaneous strict data protections, US technology companies may wish to avoid stringent ethical principles that conflict with making profits, compared to the European technological industry.[82]

The *co-regulation* approach to AI governance presents a hybrid legislative model in which statutory regulations are reinforced by ethical AI frameworks, creating a dual-layered system of compliance and accountability. Ethical AI frameworks function as normative guidelines that articulate fundamental principles of fairness, accountability, and transparency while also offering industry best practices and audit mechanisms to ensure responsible AI deployment. These frameworks, though non-binding in a strict legal sense, serve as a crucial complement to statutory regulation by fostering a culture of ethical AI development and mitigating potential legal risks. The European Commission's ethical AI framework, structured around the triad of *fairness, accountability, and transparency*, exemplifies a regulatory philosophy that seeks to embed ethical values into the foundational architecture of AI systems. By prioritizing these principles, co-regulation proponents argue that businesses and institutions can build consumer trust, promote sustainable AI innovation, and align technological progress with public interest imperatives.

A defining characteristic of this approach is the emphasis on *stakeholder participation* in shaping AI regulatory discourse. Ethical AI principles, when incorporated into legislative and governance frameworks, facilitate a multi-stakeholder engagement process involving regulators, industry leaders, civil society organizations, and academic institutions. This collaborative regulatory paradigm acknowledges that AI, as a transformative force, has implications that extend beyond legal liability into broader societal, economic, and ethical dimensions. The integration of ethical principles into AI legislation, particularly in data protection regimes, reflects a proactive recognition of AI's potential to erode privacy rights. The GDPR, for example, already encapsulates ethical considerations through its stringent data governance provisions, reinforcing the notion that AI regulation should align with pre-existing privacy frameworks to ensure consistency and coherence in legal enforcement.[83]

Despite the apparent alignment of ethical AI principles with privacy-centric legal reforms, divergences in regulatory philosophy persist across jurisdictions. The European Union's AI strategy reflects a commitment to harmonizing AI leadership with rigorous data protection measures, underscoring the belief that ethical AI governance enhances, rather than impedes, technological competitiveness. In contrast, the United States' regulatory approach remains more market-driven, with technology corporations often resistant to stringent ethical mandates that may constrain profit-maximizing AI applications. This divergence reflects a broader ideological schism between regulatory conservatism, which prioritizes economic incentives and industry autonomy, and proactive governance models that foreground privacy rights, consumer protections, and ethical AI design.

The co-regulation model, if effectively implemented, offers a promising pathway for balancing AI innovation with legal and ethical safeguards. However, its success hinges on the enforceability and uniformity of ethical AI principles across different legal systems and market environments. While voluntary ethical frameworks provide valuable normative guidance, their impact remains limited unless reinforced by legal accountability mechanisms and independent oversight bodies. Without binding obligations, ethical AI principles risk being reduced to corporate self-regulation, allowing companies to selectively adhere to guidelines without substantive compliance. Thus, a robust AI governance framework must integrate ethical principles with enforceable legal provisions, ensuring that ethical AI is not merely an aspirational goal but a regulatory reality.

---

[81] Dinesh Kumar, *Ethical and Legal Challenges of AI in Marketing: An Exploration of Solutions* 14 (Mar. 22, 2023), https://ssrn.com/abstract=4396132.
[82] Musch et al., *supra* note 79, at 5.
[83] Regulation 2016/679, *supra* note 54.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

6. CONCLUSION

In this paper, we explored the intertwined role of legislation in enhancing the principles of AI and privacy, arguing that existing laws have done much in extending long-held privacy principles to AI usage, but that there are some hurdles still to overcome. We documented some of the limitations of AI for protecting privacy when it comes to receiving meaningful consent from individuals, and we provide an analysis of metadata for robust identification. We assert that there is a role for legislation to step into the breach and up the ante for privacy protection in AI systems. A major theme of our paper is the fact that AI and legislative solutions are inextricably linked. In fact, predominantly, legislative solutions need to be legislated in such a way that they can be technically built. Legislative measures and technological measures will thus have a continuous back and forth in development to ensure that seriously privacy-invasive uses are mitigated, if not eliminated outright, over time.

A central argument advanced in this discussion is the reciprocal and evolving interplay between legislative and technological solutions. The notion that privacy laws inevitably lag behind technological advancements is a reductive perspective that fails to acknowledge the iterative nature of regulatory adaptation. Rather than treating law as an inherently reactive instrument, the emphasis must be placed on *legislative agility*—a framework in which legal principles evolve in tandem with AI capabilities. This requires an ongoing regulatory dialogue that is both anticipatory and responsive, ensuring that privacy-invasive AI applications are systematically mitigated, if not outright precluded, over time. The interplay between statutory mandates and technical feasibility must be a continuous process, where legislation is crafted with a keen awareness of its practical implementation within AI architectures, and technological development remains cognizant of emerging regulatory imperatives.

The success of AI privacy governance depends on sustained collaboration between policymakers, technology companies, and civil society. Regulatory interventions cannot exist in isolation; they must be complemented by industry best practices, technological safeguards, and public discourse to ensure that AI privacy principles are embedded within both legal and environmental frameworks.[84] The role of private-sector actors in co-developing privacy-centric AI solutions is particularly critical, as they hold the technical expertise and infrastructural capacity to translate regulatory mandates into actionable safeguards. Similarly, the participation of legal scholars, ethicists, and public interest groups is essential to shaping a balanced and rights-driven regulatory architecture.

The research trajectory that emerges from this discourse is one of perpetual refinement. AI privacy governance is not a static endeavor but a dynamic challenge that necessitates continuous legal scrutiny and technological innovation. The intersection of legal and technical feasibility remains in flux, requiring rigorous academic inquiry, policy experimentation, and empirical validation to determine what constitutes an effective and enforceable AI privacy framework. As AI continues to evolve, so too must the regulatory mechanisms that govern it, ensuring that legal safeguards do not merely react to technological disruptions but proactively shape the trajectory of AI in a manner that upholds fundamental privacy rights.

There is a strong need for ongoing collaboration between policymakers and private companies responsible for developing and rolling out AI, and candid public debate about how principles should be environmentally embedded.[85]

---

[84] See generally, Wael Armouti & Mohammad Nsour, Data Exclusivity for Pharmaceuticals in Free Trade Agreements: Models in Selected United States Free Trade Agreements, 40 Hous. J. Int'l L. 105, 105 (2017). Wael Armouti & Mohammad F. A. Nsour, Test Data Protection: Different Approaches and Implementation in Pharmaceuticals, 20 Marq. Intell. Prop. L. Rev. 267, 267 (2016). Wael Armouti & Mohammad F. A. Nsour, Data Exclusivity for Pharmaceuticals: Was It the Best Choice for Jordan under the US-Jordan Free Trade Agreement, 17 Or. Rev. Int'l L. 259, 259 (2015).

[85] For more on the use of artificial intelligence in the UAE, see Emad Abdel Rahim Dahiyat, Consumer Protection in Electronic Commerce: Some Remarks on the Jordanian Electronic Transactions Law, 34 J. Consumer Pol'y 423 (2011); Emad Abdel Rahim Dahiyat, Online Shopping and Consumer Rights in the UAE: Do We Need a Specific Law?, 33 Arab L.Q. 35 (2019); Emad Abdel Rahim Dahiyat, The Legal Recognition of Electronic Signatures in Jordan: Some Remarks on the Electronic Transactions Law, 25 Arab L.Q. 297 (2011); Emad Abdel Rahim Dahiyat, A Legal Framework for Online Commercial Arbitration in UAE: New Fabric but Old Style!, 26 Info. & Comm. Tech. L. 272 (2017); Emad Abdel Rahim Dahiyat, The Legal Recognition of Online Brokerage in UAE: Is a Conceptual Rethink Imperative?, 25 Info. & Comm. Tech. L. 173 (2016). [85] For more on the technical issues, see Saleh Al-Sharieh, The Intellectual Property Road to the Knowledge Economy: Remarks on the Readiness of the UAE Copyright Act to Drive AI Innovation, 13 L. Innovation & Tech. 141 (2021);

Research Article

Legislation is the key mode of action proposed, and suggested because updating privacy legislation with specific reference to AI and its problems would make up for gaps. The usual stance that laws will be behind the times or already overtaken by new technology is not a sufficient argument. Rather, this is a call for continuing dialogue, legislative agility, and continual monitoring and adjusting of what might be necessary within a legislative framework in response to plausible scenarios. The research gap that follows from this paper is what role legal solutions might provide, and what should be technologically feasible, are in a state of constant flux and are subject to continuous desk and field research.

REFERENCES:

[1] Azhar, Ishaq, How Artificial Intelligence Is Changing Cyber Security Landscape and Preventing Cyber Attacks: A systematic review (June 2, 2016). Ishaq Azhar Mohammed, "HOW ARTIFICIAL INTELLIGENCE IS CHANGING CYBER SECURITY LANDSCAPE AND PREVENTING CYBER ATTACKS: A SYSTEMATIC REVIEW", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.4, Issue 2, pp.659-663. Available at SSRN: https://ssrn.com/abstract=3905773

[2] Bloch, Daniel Alexandre (2018). Machine Learning: Models And Algorithms, Quantitative Analytics. Available at SSRN: https://ssrn.com/abstract=3307566

[3] Crabtree, Andy and Haddadi, Hamed and Mortier, Richard, Privacy by Design for the Internet of Things (January 6, 2022). Privacy by Design for the Internet of Things: Building Accountability and Security. The Institution of Engineering and Technology: https://shop.theiet.org/privacy-by-design-for-the-internet-of-things , Available at SSRN: https://ssrn.com/abstract=4002324

[4] Dell, S., Akpan, M., & Carr, A. (2024). Aligning artificial intelligence with ethical accountancy: A global perspective on emerging frameworks. Corporate Ownership & Control, 21(1), 47–54. P. 49. https://doi.org/10.22495/cocv21i1art5, Available at SSRN: https://ssrn.com/abstract=4721254

[5] Ebers, Martin (April 17, 2019). Chapter 2: Regulating AI and Robotics: Ethical and Legal Challenges. Algorithms and Law, Cambridge, Cambridge University Press, 2019. Available at SSRN: https://ssrn.com/abstract=3392379 or http://dx.doi.org/10.2139/ssrn.3392379

[6] ElBaih, Mohamed (April 1, 2023). The Role of Privacy Regulations in AI Development (A Discussion of the Ways in Which Privacy Regulations Can Shape the Development of AI), George Washington University, Law School. Available at SSRN: https://ssrn.com/abstract=4589207 or http://dx.doi.org/10.2139/ssrn.4589207

[7] Ellul, Joshua and Pace, Gordon J. and McCarthy, Stephen and Sammut, Trevor and Brockdorff, Juanita and Scerri, Matthew. (June 24, 2021). Regulating Artificial Intelligence: A Technology Regulator's Perspective. International Conference on Artificial Intelligence and Law ICAI. Available at SSRN: https://ssrn.com/abstract=3873329

[8] Finch, Kelsey and Tene, Omer (April 3, 2018). Smart Cities: Privacy, Transparency, and Community, Cambridge Handbook of Consumer Privacy, Eds. Evan Selinger, Jules Polonetsky and Omer Tene. Available at SSRN: https://ssrn.com/abstract=3156014

[9] Goldberg, Samuel and Johnson, Garrett and Shriver, Scott(July 17, 2019). Regulating Privacy Online: An Economic Evaluation of the GDPR .American Economic Journal: Economic Policy, 16(1): 325-58. Available at SSRN: https://ssrn.com/abstract=3421731 or http://dx.doi.org/10.2139/ssrn.3421731

[10] Goldman, Eric, An Introduction to the California Consumer Privacy Act (CCPA) (July 1, 2020). Santa Clara Univ. Legal Studies Research Paper. Available at SSRN: https://ssrn.com/abstract=3211013 or http://dx.doi.org/10.2139/ssrn.3211013

Saleh Al-Sharieh, The Regulatory Approach to Copyright Contracts Revisited: A Perspective from the UAE, 16 J. Intell. Prop. L. & Prac. 1144 (2021); Saleh Al-Sharieh, A New Copyright Law in the UAE, 17 J. Intell. Prop. L. & Prac. 214 (2022); Saleh Al-Sharieh, Competitive Advantage in the International Market of Laws: The Case of Copyright Law, 33 Info. & Comm. Tech. L. 115 (2024); Saleh Al-Sharieh, A Compliance-Driven Framework for Privacy and Security in Highly Regulated Socio-Technical Environments: An E-Government Case Study, in Research Anthology on Privatizing and Securing Data 933 (2021).

Research Article

[11] Greenleaf, Graham and Waters, Nigel and Bygrave, Lee A. (May 20, 2007). Implementing Privacy Principles: After 20 Years, it's Time to Enforce the Privacy Act. UNSW Law Research Paper No. 2007-31. Available at SSRN: https://ssrn.com/abstract=987763 or http://dx.doi.org/10.2139/ssrn.987763

[12] Jain, Sunitha Abhay, Artificial Intelligence: A Threat to Privacy? (July 26, 2019). Nirma University Law Journal: Volume-8, Issue-2. Available at SSRN: https://ssrn.com/abstract=3443004

[13] Koolen, Christof(January 24, 2020). Transparency and Consent in Data-Driven Smart Environments. European Data Protection Law Review 174 – 189. Available at SSRN: https://ssrn.com/abstract=3597736 or http://dx.doi.org/10.2139/ssrn.3597736

[14] Kumar, Dinesh (March 22, 2023). Ethical and Legal Challenges of AI in Marketing: An Exploration of Solutions. Available at SSRN: https://ssrn.com/abstract=4396132 or http://dx.doi.org/10.2139/ssrn.4396132

[15] Kuner, Christopher (February 1, 2018). International Organizations and the EU General Data Protection Regulation: Exploring the Interaction between EU Law and International Law. University of Cambridge Faculty of Law Research Paper No. 20/2018 , , 16 International Organizations Law Review 158-191. Available at SSRN: https://ssrn.com/abstract=3050675 or http://dx.doi.org/10.2139/ssrn.3050675

[16] Maas, Matthijs M. (June 16, 2021).Aligning AI Regulation to Sociotechnical Change). In: Justin Bullock, Baobao Zhang, Yu-Che Chen, Johannes Himmelreich, Matthew Young, Antonin Korinek & Valerie Hudson (eds.). Oxford Handbook on AI Governance (Oxford University Press, 2022 forthcoming). Available at SSRN: https://ssrn.com/abstract=3871635 or http://dx.doi.org/10.2139/ssrn.3871635

[17] Maas, Matthijs M. (October 25, 2023). AI is Like… A Literature Review of AI Metaphors and Why They Matter for Policy, AI Foundations Report 2. Available at SSRN: https://ssrn.com/abstract=4612468 or http://dx.doi.org/10.2139/ssrn.4612468

[18] Mahari, Robert and Pentland, Alex (2024). Regulation by Design: A New Paradigm for Regulating AI Systems Franzosi, M., Pollicino, O., & Campus, G. (Eds.). Digital Single Market and Artificial Intelligence: AI Act and Intellectual Property in the Digital Transition. Aracne. P. 432. Available at SSRN: https://ssrn.com/abstract=4753029

[19] Manheim, Karl M. and Kaplan, Lyric, Artificial Intelligence: Risks to Privacy and Democracy (October 25, 2018). 21 Yale Journal of Law and Technology 106, Loyola Law School, Los Angeles Legal Studies Research Paper No. 2018-37. Available at SSRN: https://ssrn.com/abstract=3273016

[20] Musch, Sean and Borrelli, Michael and Kerrigan, Charles (August 23, 2023). The EU AI Act: A Comprehensive Regulatory Framework for Ethical AI Development. Available at SSRN: https://ssrn.com/abstract=4549248 or http://dx.doi.org/10.2139/ssrn.4549248

[21] Ohm, P. (2014). Changing the Rules: General Principles for Data Use and Analysis. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (pp. 96–111). chapter, Cambridge: Cambridge University Press.

[22] Shumba, A.-T., Montanaro, T., Sergi, I., Fachechi, L., De Vittorio, M., & Patrono, L. (2022). Leveraging IoT-Aware Technologies and AI Techniques for Real-Time Critical Healthcare Applications. *Sensors*, *22*(19), 7675.P. 7. https://doi.org/10.3390/s22197675

[23] Tripathi, Keyur and Mubarak, Usama, Protecting Privacy in the Era of Artificial Intelligence (March 24, 2020). Available at SSRN: https://ssrn.com/abstract=3560047 or http://dx.doi.org/10.2139/ssrn.3560047

[24] Robert Walters, Matthew Coghlan. (2029). Data Protection and Artificial Intelligence Law: Europe Australia Singapore - An Actual or Perceived Dichotomy. American Journal of Science, Engineering and Technology. Vol. 4, No. 4, pp. 55-65. P. 55. doi: 10.11648/j.ajset.20190404.11

[25] Puaschunder, Julia M (2019). The Legal and International Situation of AI, Robotics and Big Data With Attention to Healthcare. Report on behalf of the European Parliament European Liberal Forum. Available at SSRN: https://ssrn.com/abstract=3472885 or http://dx.doi.org/10.2139/ssrn.3472885

[26] Robert Walters, Matthew Coghlan (2019). Data Protection and Artificial Intelligence Law: Europe Australia Singapore - An Actual or Perceived Dichotomy. American Journal of Science, Engineering and Technology. Vol. 4, No. 4, pp. 55-65. doi: 10.11648/j.ajset.20190404.11

[27] S, Anusha(November 21, 2021). Basic of Artificial Neural Network Overview. page no:87-90 CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES Volume: 02 Issue: 11. Available at SSRN: https://ssrn.com/abstract=3971265

Research Article

[28] Shomal Zadeh, Sara and Aalipour birgani, Sina and Khorshidi, Meisam and Kooban, Farhad(2023). Concrete Surface Crack Detection with Convolutional-based Deep Learning Models (November 1, 2023). International Journal of Novel Research in Civil Structural and Earth Sciences, Vol. 10, Issue 3, pp: (25-35). P. 25. Available at SSRN: https://ssrn.com/abstract=4661249 or http://dx.doi.org/10.2139/ssrn.4661249

[29] Wagner, Paul(December 8, 2020). Cookies: Privacy Risks, Attacks, and Recommendations. University of Arizona: College of Applied Science and Technology. P. 2. Available at SSRN: https://ssrn.com/abstract=3761967 or http://dx.doi.org/10.2139/ssrn.3761967

[30] Wodi, Alexander, The EU General Data Protection Regulation (GDPR): Five Years After and the Future of Data Privacy Protection in Review (2023). Available at SSRN: https://ssrn.com/abstract=4601142 or http://dx.doi.org/10.2139/ssrn.4601142

[31] Wolff, Josephine and Lehr, William and Yoo, Christopher S(August 1, 2023). Lessons from GDPR for AI Policymaking. Virginia Journal of Law & Technology, Vol. 27, art. no. 4, 2024, U of Penn Law School, Public Law Research Paper No. 23-32. Available at SSRN: https://ssrn.com/abstract=4528698 or http://dx.doi.org/10.2139/ssrn.4528698

[32] Yin, Mingqi and Cui, Xiaole and Wei, Feng and Liu, Hanqing and Jiang, Yuanyuan and Cui, Xiaoxin (2024). A Reconfigurable Fpga-Based Spiking Neural Network Accelerator. P. 1. Available at SSRN: https://ssrn.com/abstract=4876812 or http://dx.doi.org/10.2139/ssrn.4876812